This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for synchronizing a cryptosystem in a wireless communication system, the method comprising:

processing a message for transmission, wherein the message for transmission includes control data and payload data, and wherein the control data is not encrypted and contains a particular control message, and wherein the particular control message is used to provide at least one other control function;

detecting the particular control message;

based on the detecting step, determining the number of control message bytes to be transmitted, loading an encryption synchronization counter with the number of control message bytes to be transmitted and initializing the encryption synchronization counter;

when the encryption synchronization counter is decremented to zero, initializing the cryptosystem using a key;

using the cryptosystem to encrypt the payload data;

creating an encrypted airlink packet for transmission over an airlink;

receiving a message, including unencrypted control data and encrypted payload data, over the airlink;

parsing the received message to separate the unencrypted control data from the payload data;

determining whether the control data contains the particular unencrypted control message;

if the unencrypted control data contains the particular unencrypted control message, initializing the cryptosystem using the key; and

using the cryptosystem to decrypt the received payload data.

2. (Original) The method of claim 1, wherein the particular control message is a final link control channel ("LCC") message transmitted before the transmission of payload data begins, and wherein transmission of the final link control channel occurs each time a call over an airlink channel is set up.

3. (Original) The method of claim 1, wherein initializing the cryptosystem includes operating on a state box using the key.

4. (Original) The method of claim 1, wherein initializing the cryptosystem comprises:

performing a mathematical operation on the key to alter the key for security, wherein the key is an array of data; and

operating on a state box using the altered key, wherein the state box is an array of data.

5. (Original) The method of claim 1, wherein the cryptosystem includes an RC4 state box and an RC4 key, and wherein the payload data is operated on using the RC4 state box for encryption and decryption.

6-17. (Canceled)

18. (Previously Presented) A computer-readable medium whose contents cause a transmitter in a communications system to perform a method for synchronizing encryption and/or decryption of transmitted data, the method comprising creating a packet for transmission over a link, including:

sending messages for transmission in blocks of data from a central processing unit ("CPU") to a communication link digital signal processor;

detecting a particular unencrypted control message within unencrypted control data that passes unencrypted through an associated control channel for initiating encryption, wherein the particular control message is used according to a wireless communication protocol to provide at least one other control function under the wireless communication protocol;

in response to detecting, determining a size of the control data, loading the size of the control data into a counter, wherein the counter decrements when each portion of the control data is sent;

when the counter reaches zero, initiating an encryption and/or decryption synchronization process within the associated control channel, including generating a state box using an encryption key; and

encrypting transmissions following the control message for transmission for the packet.

19. (Previously Presented) The computer readable medium of claim 18, wherein the method further comprises creating a control message packet for sending to the CPU, including,

receiving an airlink packet;

parsing the airlink packet to separate payload data from control data;

detecting a particular control message in the airlink packet;

in response to detecting, initiating an encryption and/or decryption synchronization process, including generating a state box using an encryption key; and decrypting data following the particular control message.

20. (Original) The computer readable medium of claim 18, wherein the packet comprises the encryption key.

21. (Previously Presented) The computer readable medium of claim 18, wherein initiating the encryption and/or decryption synchronization process further includes changing the encryption key according to a predetermined algorithm, and operating on the state box using the changed encryption key.

22. (Original) The computer readable medium of claim 18, wherein the method is performed at an associated control channel level of processing.

23. (Previously Presented) The computer readable medium of claim 18, wherein the method is performed each time a base station participates in setting up an airlink channel.

24. (Previously Presented) The computer readable medium of claim 18, wherein the particular control message is a link control channel ("LCC") message that is a "set asynchronous balance mode" ("SABM") message or a "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") message.

25. (Previously Presented) An apparatus for synchronizing an encryption and/or decryption process in a wireless communication network, comprising:

at least one digital signal processing means;

at least one central processing means; and

encryption synchronization means configured to detect a particular unencrypted control message in an unencrypted control data portion of a data transmission, wherein the particular unencrypted control message is used according to a wireless communication protocol to provide at least one other control function under the wireless communication protocol, and, in response, initiate an encryption and/or decryption process, wherein the particular unencrypted control message occurs just before the transmission of telephony data and wherein further the encryption synchronization means and the encryption and/or decryption process operates at an associated control channel level in the wireless communication network.

26. (Original) The apparatus of claim 25, wherein the encryption synchronization means is further configured to provide a current encryption key to receiving devices and sending devices in the wireless communication network.

27. (Previously Presented) The apparatus of claim 25, wherein the encryption synchronization means is further configured to count control data blocks in a message being transmitted and compare that count to the total number of control data blocks to determine when to begin encryption and/or decryption.

28. (Original) The apparatus of claim 26, wherein initiating the encryption/decryption process comprises using the current encryption key to generate a current state box, wherein the current state box is used to operate on the telephony data.

29. (Canceled)

30. (Previously Presented) The apparatus of claim 25, wherein the initiation of the encryption and/or decryption process occurs each time a wireless connection is set up, comprising initial connection, connection hand off, and connection reestablishment after unexpected connection loss.

31-33. (Canceled)